

METHODS AND APPARATUS FOR ACCELERATING ARC4 PROCESSING

Abstract of the Disclosure

5

Methods and apparatus are provided for improving ARC4 processing in a cryptography engine. A multiple ported memory can be used to allow pipelined read and write access to values in memory. Coherency checking can be applied to provide that read-after-write and write-after-write consistency is maintained. Initialization of the memory can be improved with a reset feature occurring in a single cycle. Key shuffle and key stream generation can also be performed using a single core.

10

100221 60192001